REMARKS

The Examiner has rejected Claims 13-15, 19-21, 41, and 42 under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. More specifically, the Examiner has stated that "[t]he instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process." Additionally, the Examiner has argued that "[t]he key updating method including steps of updating a key based on a user eviction is broad enough that the claim could be completely performed mentally, verbally or without a machine nor is any transformation apparent."

Applicant respectfully disagrees. "A claimed process is surely patent-eligible under §101 if: (1) it is tied to a particular machine or apparatus, or (2) it transforms a particular article into a different state or thing," where the transformed articles may include "physical objects or substances" or articles "representative of physical objects or substances." *In re Bilski*, 545 F.3d 943, 954 & 963 (Fed. Cir. 2008)

In the present case, applicant claims "**determining** an updated first key" (emphasis added), as claimed, which is a "transformation" and is clearly statutory. By virtue of the claimed "determining," as claimed, applicant clearly teaches and claims a "transformation" of a physical object or substance, or an article representative of a physical object or substance, to a different state or thing.

For these and various other reasons, applicant respectfully contends that the claims at issue are clearly statutory and meet the requirements of 35 U.S.C. 101.

Nevertheless, applicant has amended independent Claim 13 to further avoid the above rejection.

The Examiner has rejected Claims 13-15, 19-21, 41-45, and 48-50 under 35 U.S.C. 102(b) based upon a public use or sale of the invention. Specifically, the

Examiner has argued that "the invention of the instant application was publicly used more than one year prior to the Applicant's filing for invention, as can be seen by **Dynamic Cryptographic Context Management (DCCM): Report #1 Architecture and System Design**, which was first published on 02 June 1998." Applicant respectfully disagrees with such rejection for at least the reasons illustrated below that clearly distinguish applicant's claimed language from the aforementioned reference.

The Examiner has rejected Claims 13-15, 19-21, 41-45, and 48-50 under 35 U.S.C. 102(b) as being anticipated by Balenson et al. ("Dynamic Cryptographic Context Management (DCCM): Report #1 Architecture and System Design"). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to the independent claims. Specifically, applicant has amended the independent claims to at least substantially include the subject matter of Claim 42.

With respect to the independent claims, the Examiner has relied on Pages 34, 47, 54, and 99 from the Balenson reference to make a prior art showing of applicant's claimed technique "wherein said determining uses a function having the following properties: (1) knowledge of said updated first key does not give knowledge of said first key or said second key,...and (3) knowledge of said first key and said updated first key does not give any knowledge of said second key" (see the same or similar, but not necessarily identical language in each of the independent claims). More specifically, the Examiner has asserted that the above reference excerpts "provid[e] a showing of the properties as backward secrecy, forward secrecy, and collusion-resistance."

Applicant respectfully points out that the Balenson reference excerpts relied upon by the Examiner merely teach that "[i]f a private key is compromised, all digital certificates containing the matching public key must be revoked" and that "[t]his is reported back to the certificate server where the on-line certificate repository is updated" (Page 34, first paragraph – emphasis added). The excerpts further teach that "[s]ecret keys have to be transmitted... in a confidential manner such that they cannot be modified or replaced by another key in an unauthorized and undetected manner" and that "[k]eys

have to be... protected in a user-friendly and failsafe manner" (Page 34, fourth and fifth paragraphs – emphasis added).

Additionally, the excerpts from Balenson teach "encrypt[ing] the data," "detection mechanisms [that] serve to reduce the probability of compromise," and "[a] trust model" (Page 47, second and third paragraphs – emphasis added). Further, the excerpts disclose that "the enrollment process establishes for each member an *individual DCCM base key* known only to the member and his enrolling DCCM manager" and that "these DCCM base keys allow for certain efficiencies in establishing individual group base keys" (Page 54, second paragraph – emphasis added), in addition to "establishing for each group member an individual group base key known only to the member and the group manager" and "repeat[ing] a pair-wise authenticated key exchange protocol separately for each group member" (Page 54, third paragraph – emphasis added).

Further still, the aforementioned excerpts teach that "in order to prevent collusion by two or more evicted members, a large amount of information must be predistributed" (Page 99, ninth paragraph -emphasis added). In particular, such excerpt from Balenson discloses that "[w]hen a member is evicted, the remaining group members can use this predistributed information to compute a new key, without any trusted controller separately transmitting the new key" (Page 99, ninth paragraph - emphasis added).

However, applicant respectfully asserts that generally disclosing revoking digital certificates with a public key if a matching private key is compromised, protecting keys and transmitting keys in a confidential manner, encrypting data, utilizing detection mechanisms and a trust model, establishing a base key known only to a member and an enrolling manager, in addition to disclosing that "a large amount of information must be predistributed," such that "remaining group members can use this predistributed information to compute a new key," as in Balenson, does not teach that "said determining uses a function having the following properties: (1) knowledge of said updated first key does not give knowledge of said first key or said second key," and "(3) knowledge of said

first key and said updated first key does not give any knowledge of said second key," as specifically claimed by applicant.

In particular, simply disclosing the revoking of a public key if the matching private key is compromised, encrypting data and establishing a base key known only to a member and an enrolling manager, as well as the use of predistributed information to compute a new key, as in Balenson, does not suggest, and especially does not rise to the level of specificity of, applicant's claim language, namely that "knowledge of said updated first key does not give knowledge of said first key or said second key...and...knowledge of said first key and said updated first key does not give any knowledge of said second key" (emphasis added), as claimed.

In the Office Action mailed 12/17/2007, the Examiner has cited *Texas Instruments Inc. v. U.S. International Trade Commission* and has argued that "[t]he Examiner has afforded the [aforementioned] limitation very little patentable weight since wherein clauses in method claims are not given weight when they simply express the intended result of a process step positively recited." Additionally, the Examiner has cited *Minton v. National Association of Securities Dealers, Inc.* and has argued that "[i]n this case the wherein clause merely expresses properties that result from the determining step" and that "the properties disclosed in the wherein clause do not provide any information regarding the mechanics of how the determining step is executed."

Applicant respectfully disagrees. Applicant respectfully asserts that, when taken in context, applicant claims that "said determining [an updated first key] uses a function having the following properties to determine the updated key: (1) knowledge of said updated first key does not give knowledge of said first key or said second key, (2) knowledge of said first key does not give any knowledge of said updated first key, and (3) knowledge of said first key and said updated first key does not give any knowledge of said second key" (see Claim 1 – emphasis added), and "said key server using a function having the following properties to determine the updated key: (1) knowledge of said updated first key does not give knowledge of said first key or said second key, (2)

knowledge of said first key does not give any knowledge of said updated first key, and (3) knowledge of said first key and said updated first key does not give any knowledge of said second key" (see Claim 43 – emphasis added), which clearly do not simply "express properties that result from the determining step" (emphasis added), as suggested by the Examiner.

Additionally, in the Office Action mailed 12/17/2007, the Examiner has argued that "the Applicant never states that the properties are not for the collusion resistance and merely argues that the reference is not as specific as the claim language." The Examiner has further argued that "[t]his amounts to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references, especially since the applicant never says that the properties are not for collusion resistance."

Applicant respectfully disagrees and again asserts that for at least the reasons noted above, Balenson does not suggest, and especially does not rise to the level of specificity of, applicant's claim language, namely that "knowledge of said updated first key does not give knowledge of said first key or said second key...and...knowledge of said first key and said updated first key does not give any knowledge of said second key" (emphasis added), as specifically claimed.

In the Office Action mailed 02/09/2009, the Examiner has merely reiterated their above arguments and has failed to specifically respond to applicant's above arguments with respect to applicant's claimed technique "wherein said determining uses a function having the following properties: (1) knowledge of said updated first key does not give knowledge of said first key or said second key,...and (3) knowledge of said first key and said updated first key does not give any knowledge of said second key." Applicant again notes that Balenson does not suggest, and especially does not rise to the level of specificity of, applicant's claim language, namely that "knowledge of said updated first key does not give knowledge of said first key or said second key...and...knowledge of said first key and said updated first key does not give any knowledge of said second key"

(emphasis added), as specifically claimed. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Additionally, with respect to the independent claims, the Examiner has relied on Page 10, Fig. 2, and Page 11, Fig. 3, specifically, "$k_i = f(k'_x, k'_y)$," of the above reference to make a prior art showing of applicant's claimed technique "wherein said updated first key is equal to F(first key, second key), wherein F() is a one-way function" (see this or similar, but not necessarily identical language in the independent claims). Additionally, in the Office Action mailed 02/09/2009, the Examiner has argued that "pages 10 and 11, figures 2 and 3, respectively, ...disclose $k_i = f(k'_x, k'_y)$ in a one-way function tree" and that "[s]ince DCCM discloses the newly added limitation in at least Figures 2 and 3, the rejection is maintained."

Applicant respectfully disagrees and notes that Fig. 2 of the above reference relied on by the Examiner merely discloses "[a] one-way function tree for establishing a group key for 8 members." However, merely disclosing a one-way function tree for establishing a group key does not teach a technique "wherein said updated first key is equal to F(first key, second key), wherein F() is a one-way function" (emphasis added), as specifically claimed by applicant.

Additionally, applicant respectfully notes that the excerpts relied on by the Examiner merely disclose "comput[ing] the node keys along the path from the leaf to the root" (Page 10 – emphasis added). Additionally, the excerpts disclose that "[e]ach node *i* has a key k_i and a blinded node key $k'_i = g(k'_i)$, where g is a one-way function," where "node keys are computed by all members 'bottom-up' using the one-way function *f*," and where "$k_i = f(k'_X, k'_Y)$," where k_X and k_Y are leaves and k_i is a node (Fig. 3 text). Further, the excerpts disclose that "one can compute a blinded key from a normal key but not vice versa," where "each node of the tree has a key which is used to communicat[e] securely with the members at the leaves below the node" (Page 10 – emphasis added).

However, merely determining a node key utilizing a function applied to two blinded node keys created from leaf keys, where the node key is used for secure communications with the members at the leaves below the node, as in Balenson, fails to disclose a technique "wherein said updated first key is equal to F(first key, second key), wherein F() is a one-way function," where the "first key... enables secure communication among a set of users," and where the "second key enables secure communication among a subgroup of said set of users, wherein said subgroup does not include users subject to said eviction" (see this or similar, but not necessarily identical language in the independent claims - emphasis added), as specifically claimed by applicant.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Balenson reference excerpts, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has incorporated the subject matter of former Claim 42 et al. into the independent claims.

With respect to the subject matter of former Claim 42 (now at least substantially incorporated into each of the independent claims), the Examiner has again failed to provide a specific prior art rejection of applicant's claimed technique "wherein said subgroup is a self-repairing group, each member of said subgroup capable of independently updating said first key, where said self-repairing uses a reusable power set, said reusable power set using a power set of said members as a basis for group key updates and including 2^N sets, where N includes the number of said members." Thus, a

notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Again, since the above anticipation criterion has simply not been met by the Balenson reference excerpts, as noted above, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to dependent Claims 14 and 15 et al., the Examiner has relied on Page 115, Fig. 29 to make a prior art showing of applicant's claimed technique "wherein only said second user is evicted" (see Claim 14 et al.) and "wherein said second user and one or more other users in said set of users are evicted" (see Claim 15 et al.).

Applicant respectfully notes that the above reference excerpt relied on by the Examiner merely discloses the "Blinded ancestral sibling nodes of a CAT." However, nowhere in the above reference excerpt is a technique taught "wherein only said second user is evicted" (see Claim 14 et al. – emphasis added) or "wherein said second user and one or more other users in said set of users are evicted" (see Claim 14 et al. - emphasis added), as claimed by applicant.

In the Office Action mailed 02/09/2009, the Examiner has failed to specifically respond to applicant's above arguments with respect to applicant's claimed techniques "wherein only said second user is evicted" (see Claim 14 et al.) and "wherein said second user and one or more other users in said set of users are evicted" (see Claim 15 et al.). Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Additionally, with respect to dependent Claims 19 and 48, the Examiner has relied on Page 10, Fig. 2 to make a prior art showing of applicant's claimed technique

"wherein said determining uses only said first key and said second key" (see the same or similar, but not necessarily identical language in the aforementioned claims). More specifically, the Examiner has argued that "binary trees only account for two child nodes."

Applicant disagrees and again respectfully notes that the above reference excerpt relied on by the Examiner merely discloses "[a] one-way function tree for establishing a group key for 8 members." However, merely disclosing a one-way function tree for establishing a group key does not teach a technique "wherein said determining [an updated first key] uses only said first key and said second key" (emphasis added), in the context specifically claimed by applicant (see independent claims for context).

In the Office Action mailed 02/09/2009, the Examiner has failed to specifically respond to applicant's above arguments with respect to applicant's claimed technique "wherein said determining uses only said first key and said second key" (see the same or similar, but not necessarily identical language in the aforementioned claims). Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Yet again, since the above anticipation criterion has simply not been met by the Balenson reference excerpts, as noted above, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 51-52 below, which are added for full consideration:

> "wherein an artificial eviction is performed just prior to an addition of another user to said set of users" (see Claim 51); and
>
> "wherein said set of keys is modified periodically" (see Claim 52).

To this end, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P089).

Respectfully submitted,
Zilka-Kotab, PC

/KEVINZILKA/

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100